COLLEGE OF CREATIVE INNOVATION

Programme

Diploma in Cloud Computing and Cyber Security
(120 Credits)

Course

CCC604: Multi-Cloud Security Integration and Project Management
(Level 6, 30 Credits, Version 1.1)

Assessment Title

Project

CCC604 | Assessment-7

(Group Activity)

Weighting within the course

70%

Objective:

This assessment evaluates your ability to plan, execute, and manage a multi-cloud security project aligned with industry standards, reflecting the needs of the qualification by meeting the following learning outcomes **(LO2, LO3, LO4, and LO6)** and Graduate Profile Outcomes **(GPO5, GPO6, and GPO7)**. It demonstrates your capacity to apply project management principles, evaluate security tools for diverse multi-cloud environments, develop risk assessment and mitigation strategies, and analyse security incidents and vulnerabilities to troubleshoot within cloud services. Through this, you will show professional and ethical practices **(GPO5)**, apply effective communication and teamwork skills **(GPO6)**, and use project management tools and critical thinking to solve IT-related problems **(GPO7)** in support of secure, robust multi-cloud deployments.

Course Learning Outcomes (LOs) covered:

LO2: Apply project management principles to plan, execute, and oversee a multi-cloud security project to meet industry standards. **(GPO5)**
LO3: Evaluate relevant security tools and technologies for diverse multi-cloud environments **(GPO6)**
LO4: Develop a comprehensive risk assessment and mitigation strategy specific to multi-cloud deployments. **(GPO6)**
LO6: Analyse security incidents and vulnerabilities to troubleshoot within cloud services. **(GPO7)**

Qualification Graduate Profile Outcomes (GPOs) covered:

GPO5: Apply professional and ethical practices with integrity to meet the industry wide expectations of a responsible IT professional, in accordance with legal, regulatory, and organisational requirements.
GPO6: Apply communication, information design, teamwork, personal, and interpersonal skills, to enhance working effectiveness, efficiency, and quality outcomes in a variety of situations in an organisational environment.
GPO7: Apply project management tools and techniques, critical thinking, enterprise skills and knowledge of project planning, management, and control, to analyse and solve problems for an IT related project.

Assessment Tasks to Learning Outcome and GPOs Mapping:

	Tasks	Learning Outcomes	GPOs	Weighting
Phase 1: Project Planning, Design, and Assignment of Group and Individual Roles	**Task1:** Project Planning	**LO2**	**GPO5**	**15%**
Phase 2: Multi-Cloud Project Implementation Using AWS and Azure Services, with Security Incident Identification and Troubleshooting	**Task 2: Part-A |** Project Implementation using AWS Cloud Services **Task 2: Part-B |** Project Implementation using Azure Cloud Services **Task 2: Part-C |** Multi-Cloud Security Integration	**LO2, LO3, LO4, LO6**	**GPO5, GPO6, GPO7**	**50%**
Phase 3: Risk Assessment and Security Incident Analysis	**Task 3: Part-A |** Risk Assessment and Mitigation Strategy **Task 3: Part-B |** Security Incidents Analysis	**LO3, LO4**	**GPO6**	**20%**
Phase 4: Prepare Project Documentation, Write Report, and Conduct Verification	**Task 4:** Project Documentation, Report Writing, Testing and Verification	**LO6**	**GPO7**	**15%**
				Total 100%

Recommended Tasks Completion Timeline:

Full Time Week	Part Time Week	Progress	Submission
Week 25	Week 49,50	Start working on Assessment-7 Task-1	
Week 26	Week 51,52	Complete Task-1 Project planning	
Week 27	Week 53,54	Complete Task-2 Part-A	
Week 28	Week 55,56	Complete Task-2 Part-B	
Week 29	Week 57,58	Complete Task-3	
Week 30	Week 59,60	Complete Task-4 Part-A and Part-B	
Week 31	Week 61,62	Complete Task-5 and Submission	Assessment due by Week-31 (Full Time) Assessment due by Week-62 (Part Time)

Grading:

The final grade will be determined by the score achieved in this assessment based on the following table. Should a second or third attempt be required, the maximum contribution toward the overall mark for the tasks that required a second or third assessment attempt is 50%. **A late submission is considered a second attempt, so the contribution will be capped at 50%.**

To pass this assessment, you must meet the requirements of each of the learning outcomes (irrespective of the numerical grade awarded).

Grade	Range
A	Meet all course requirements, range (80—100%)
B	Meet all course requirements, range (65—79%)
C	Meet all course requirements, range (50—64%)
D	Did not meet all course requirements, range (40—49%)
E	Did not meet all course requirements, mark range (0—39%)

Candidate's Assessment Instructions:

- This assessment is an **open-book activity**, you can use your course and review notes, and offline or online resources, such as textbooks or online journals.
- You can always ask your online tutor if you need further explanation if the instructions are unclear.
- Your work should not be plagiarised. Plagiarism includes copying material without acknowledging it, copying from another student, getting another person to help you with your assessment, using material from commercial essays or assignment services, or using AI to create the answers.
- The purpose of this assessment is to assess your knowledge. In the event Yoobee suspects collusion, this will be addressed. For more information on plagiarism, please refer to the Student Handbook.
- Submit your completed assessment online in the correct space provided.
- Marks and feedback will be returned within 15 days of the submission date.
- By completing and submitting an assessment you are authenticating that the work is original and does not violate plagiarism or copyright law. Authenticity is checked where any breaches of academic integrity are suspected. Please refer to the Student Handbook for further information.

Submission Instructions:

Submit **one PDF report** document to the LMS by the specified due date.

Your report should:

- Include your name and ID number
- Include the AWS account login details, a cover page, and a report index for verification purposes in your report.
- Use a standard citation format if, external sources are referenced
- Clearly label tasks and subtasks and Diagrams must be clear and labeled properly.
- Include screenshots of each practical step in sequence, naming and numbering the screenshots. Screenshots must display the relevant settings or outputs for each step.
- Include your answers to the assessment questions for each task, describing choices, configurations, and learned insights with an appropriate practical and theoretical understanding.

Assessment Tasks: Multi-Cloud Security Integration and Project Management

Scenario:

Yoobee College is undertaking a strategic migration of its existing WordPress website and supporting IT infrastructure to a multi-cloud environment. The goal is to ensure high availability, improved security, and cost efficiency by leveraging services across **AWS (Amazon Web Services), Microsoft Azure, and Fortinet FortiGate.**

As part of this assessment, you are part of the student team acting as the cloud security architects and engineers responsible for planning, implementing, securing, and documenting this migration.

You will work in a realistic, industry-inspired scenario, demonstrating your ability to design and deliver a secure, integrated multi-cloud solution that aligns with best practices. Your work will showcase practical application of project management principles, security design, tool evaluation, risk mitigation planning, and incident analysis.

Your Task:

You are required to produce a **complete Project Portfolio** documenting your team's work on this project.

Your submission will demonstrate:

- **Effective planning and management** of the migration project
- **Technical implementation** of secure AWS and Azure services, showing integration of resources
- **Integration of security tools and technologies**, including Fortinet FortiGate
- **Identification and assessment of risks** with well-defined mitigation strategies
- **Analysis of potential vulnerabilities** and a plan for **incident detection and response**

Phase 1 | Project Planning, Design, and Assignment of Group and Individual Roles

Task-1 Project Planning

Complete all sections below. Each section includes a description of what you need to write. This document is your official Project Planning submission in PDF format.

1. **Introduction to the Project and Group**

Description:
Provide a short introduction to your project. Explain what you are trying to achieve (e.g., integrating AWS and Azure securely). Include your team's name or group number and list all members with student IDs.

What to include:

- Project title
- Project summary or goal
- Group members' full names and short summary.

2. **Individual Student Responsibilities**

Description:
List each team member's assigned role and their main responsibilities in the project. This ensures everyone knows what they need to do.

What to include:

- A table with columns for Name, Role, Responsibilities.
- Example roles: Project Manager, Security Architect, Cloud Engineer.
- Clearly describe the tasks each person will handle.

3. **Project Layout and Diagram**

Description:
Create and add a high-level diagram of your planned cloud architecture. This helps visualise how AWS, Azure (or other providers) will connect and where security controls will be applied.

What to include:

- A labelled diagram (you can use Lucid chart, Draw.io etc.).
- Show major components of AWS, Azure cloud services and Fortinet configurations.
- A brief caption explaining your diagram.

4. **Step-by-Step Checklist for Timely Completion**

Description:
Outline a step-by-step list of tasks your team will complete to finish the project on time. This is your action plan.

What to include:

- Numbered or bulleted list of project steps.
- Cover planning, design, configuration, testing, documentation.
- Make sure steps are clear and in order.

5. **Project Submission Guidelines**

Description:
Explain how your team will ensure your final project meets the submission requirements. Include details of the format, contents, and platform for submission.

What to include:

- File format (e.g., single PDF).
- Required contents (diagram, documentation, screenshots).
- Due date or timeline.
- Any academic integrity or citation notes.

6. **Project Weekly Timesheet**

Description:
Create a weekly schedule for your team to manage time effectively. This helps you stay on track.

What to include:

- A table with columns for Week, Task, Hours/Person, Notes.
- Assign approximate hours for each week.
- Include key tasks or milestones for each week.

7. **Tutor Meeting Minutes**

Description:
Record planned or past meetings with your tutor. This shows you are engaging in regular check-ins for feedback.

What to include:

- A table with columns for Date, Attendees, Summary of Discussion, Action Items.
- Summarise each meeting’s outcomes and next steps.
- Leave blank rows for future meetings if needed.

8. **Define Project Scope and Objective**

Description:
Clearly state what your project will cover (scope) and what you aim to achieve (objectives). This section sets boundaries and goals for your work.

What to include:

- Scope: Specific areas your project will address (e.g., IAM design, encryption, logging, multi-cloud integration).
- Objectives: Clear, measurable goals (e.g., implement IAM roles, enable encryption at rest/in transit, centralised logging).

9. **Risk Management Approach**

Description:
Identify potential risks that could affect your project and explain how you will manage or reduce them. This shows you have a plan to deal with problems.

What to include:

- Risk identification: List of possible issues (e.g., configuration errors, time overruns).
- Mitigation strategies: How you’ll avoid or respond to each risk (e.g., peer reviews, templates, backup plans).

10. Communication Strategy

Description:
Explain **how your team will communicate and coordinate** during the project. Clear communication prevents mistakes and delays.

What to include:

- Frequency of meetings (e.g., weekly).
- Tools you will use (e.g., Microsoft Teams, Google Docs etc..).
- How you will share updates and track progress.
- How you will keep your tutor informed.

Deliverables:

- Complete all sections with **clear and specific answers**.
- Use clear tables and headings to make your document easy to read.
- Include your **architecture diagram**.
- Export the document as **PDF**.

Note:

This planning document serves as your **blueprint** for the entire project. It will guide your team's work during implementation. Your tutor may review it and provide feedback to help you **refine and improve your plan** before you begin building your solution.

Phase 2 | Multi-Cloud Project Implementation Using AWS and Azure Cloud Services, with Security Incident Identification and Troubleshooting

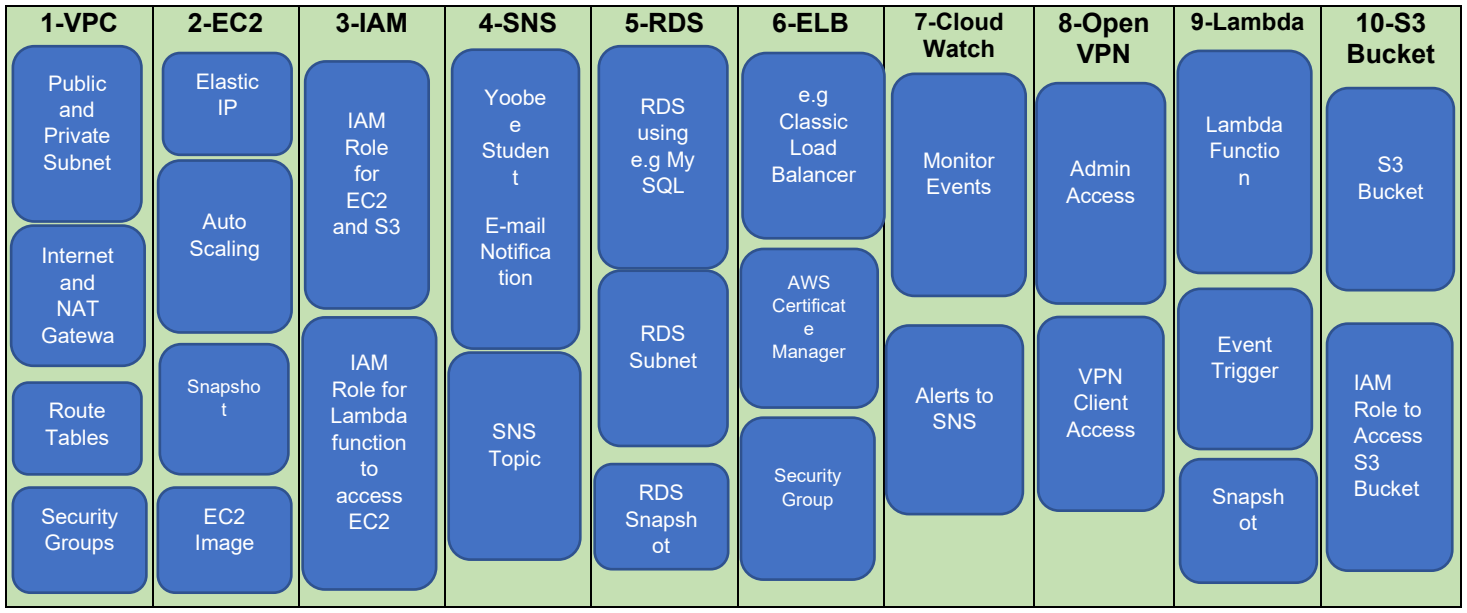
All students have developed knowledge of Amazon Web Services (AWS), Microsoft Azure, and Fortinet security management throughout the *Diploma in Cloud Computing and Cyber Security* course from **Weeks 1 to 24 for full-time** students, and **Weeks 1 to 48 for part-time** students. This assessment is designed to let you apply these skills by using AWS, Microsoft Azure, and Fortinet services to **design, implement, and present a secure, multi-tier, multi-cloud architecture project**.

Yoobee College of Creative Innovation has decided to migrate its on-premises web-based infrastructure (WordPress website) to a multi-cloud architecture using Microsoft Azure and Amazon Web Services (AWS) by implementing cloud-based security using Fortinet. This migration aims to enhance security, monitoring, and high availability while utilizing a range of cloud services. The current on-premises infrastructure includes the following key services:

1. **Active Directory Domain Services (ADDS):** Manages user accounts for staff and students.
2. **Domain Name System (DNS):** Maintains all web-based applications through domain name resolution.
3. **Dynamic Host Configuration Protocol (DHCP):** Assigns automatic IP addresses to staff and student computers, including BYOD devices.
4. **File Transfer Protocol (FTP):** Stores and transfers files, supported by Network-Attached Storage (NAS) for centralized data storage.
5. **Web Server:** Hosts and provides access to all applications using a Microsoft-based web server.
6. **SQL Server:** Manages back-end databases, with a web-based front-end for applications.
7. **Virtual Private Network (VPN):** Ensures secure remote access and management with Windows Certificate Authority integration.
8. **Windows Server 2016 Certificate Authority:** Maintains web server security and authentication.
9. **Group Policy Management:** Centralizes configuration and management of operating systems, applications, and user settings in an Active Directory environment.
10. **Windows Server 2016 Monitoring Services:** Includes tools like Event Viewer and Performance Management for system monitoring and maintenance.

This migration will leverage cloud-based solutions to enhance scalability, reliability, and security while ensuring a seamless transition from the existing infrastructure.

Task 2: Part-A | Project Implementation using AWS Cloud Services

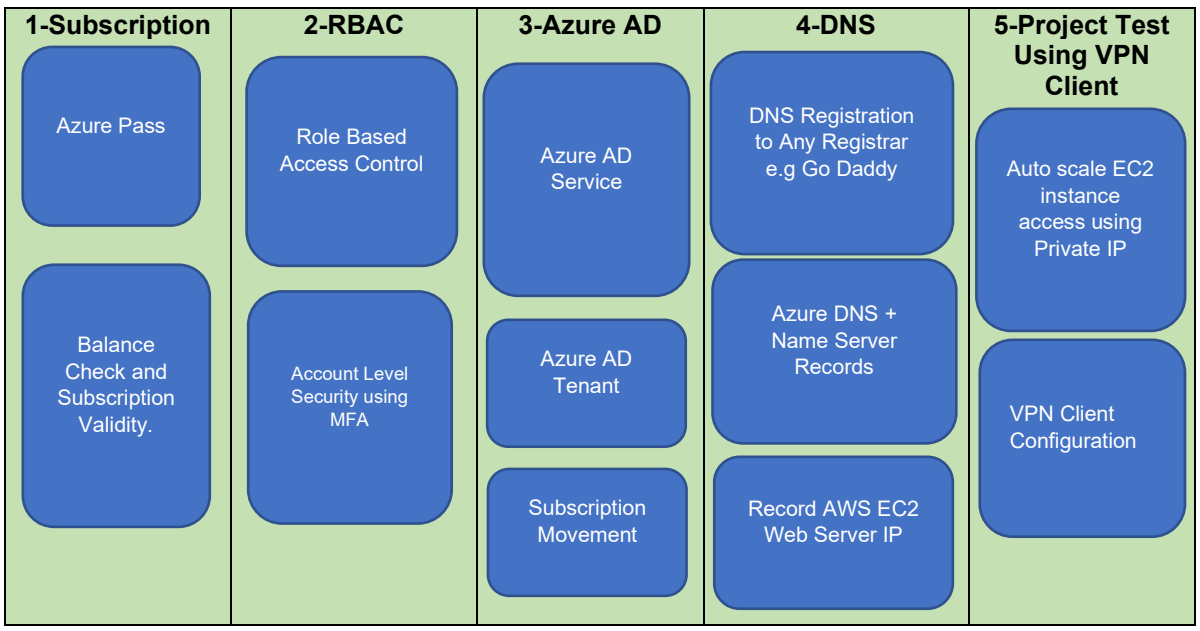


Deliverables:

Important Note: Tag should be provided as Key = **Group Name-Number (e.g Groupname21)** Value = **Identity of resource**

1. VPC: Virtual Private Cloud with your own design infrastructure including Public and Private Subnets, Internet Gateway, Route table, NAT Gateway, Elastic IP address and other require VPC components.
2. EC2: Elastic Compute Cloud. You must use Amazon Linux instance as a server (Front-End) and require security group with port number.
3. IAM: Identity and Access Management Service.
4. SNS: Simple Notification Service received by Yoobee student E-mail (One student E-mail from Group)
5. RDS: Relational Database Service (My SQL or any suitable server as Back-End)
6. ELB: Elastic Load Balancer including ACM (Amazon Certificate Manager with SSL Certificate to secure environment) and Autoscaling to provide high availability to your word press web application.
7. Cloud Watch: Monitor your web server event pattern running and stopping and notified by SNS
8. VPN: Virtual Private Network (Use Open VPN free tier service) to connect your Front-End web server generated by Auto Scaling using Private IP address to perform certain modification.
9. Lambda: Research a code or Write function to create a snapshot of your EC2 web server instance using Lambda service also, in timely manner to Trigger function and automatically create snapshot every day.
10. S3: Use S3 bucket for snapshot created in step-9 to store backups as instance snapshot.

Task 2: Part-B | Project Implementation using Azure Cloud Services



Project Implementation Guidelines:

1. **Subscription:**
    - A Microsoft Azure subscription is required from one of your group members' logins to utilise Azure cloud services. You can make a new account with credit provided by Microsoft for a month.
2. **RBAC (Role-Based Access Control):**
    - Implement Microsoft Azure Account Security using Multi-Factor Authentication (MFA).
    - Assign appropriate role-based permissions to ensure controlled access.
3. **Azure AD (Active Directory):**
    - Create a tenant with the name (Your Group Name) to manage authentication and authorization for Azure services, including subscription access.
4. **DNS (Domain Name System):**
    - Integrate AWS Services with Microsoft Azure DNS to enable name resolution for your WordPress website.
5. **Project Testing:**
    - Validate project functionality using VPN Client Service.
    - Ensure secure access via HTTPS and test web server connectivity.
    - Deliverables:

Deliverables:

By the end of the implementation, your WordPress website must be securely accessible via HTTPS from any location using the DNS service name records in Microsoft Azure.

Task 2: Part-C | Multi-Cloud Security Integration

In this task, you will design, implement, and document the security aspects of your multi-cloud project with a focus on AWS and Fortinet FortiGate integration.

You will demonstrate your ability to plan and configure robust security controls across AWS and Azure environments, using Fortinet solutions to ensure secure interconnectivity and traffic management

1. AWS Security Design and Implementation

- Define IAM roles, policies, and least-privilege access.
- Implement encryption (at rest and in transit) using AWS KMS.
- Configure AWS security groups and network ACLs.
- Enable and document logging/monitoring with CloudWatch and CloudTrail.
- Provide screenshots or scripts as evidence.

2. Fortinet FortiGate Integration

- Design secure inter-cloud network traffic using FortiGate.
- Configure FortiGate policies, VPN tunnels, or routing as needed.
- Document firewall rules and inspection policies for AWS and Azure connectivity.
- Include a diagram showing Fortinet's placement in your architecture.
- Provide screenshots or configuration examples.

3. Risk Assessment for Security Controls

- Identify specific risks (e.g., IAM misconfiguration, VPN exposure).
- Describe mitigation strategies (e.g., MFA enforcement, policy reviews).

Deliverables:

- Step-by-step configuration instructions.
- Screenshots of Fortinet and AWS consoles or CLI outputs.
- Diagrams illustrating security architecture.

Phase 3 | Risk Assessment and Security Incident Analysis

In this phase, your team will formally assess risks associated with your multi-cloud implementation, document mitigation strategies, and conduct a security incident analysis. This demonstrates your ability to plan for, detect, and respond to threats in a realistic environment.

Task 3: Part-A | Risk Assessment and Mitigation Strategy

Description:
Identify and document specific risks to your multi-cloud architecture, along with detailed mitigation strategies for each. Your assessment must address both AWS and Azure environments as well as inter-cloud connectivity (including Fortinet FortiGate integration).

What to Include:

- A clear table listing:
    - Risk ID or Number
    - Description of Risk (e.g., IAM misconfiguration, VPN exposure, data breach)
    - Likelihood (Low/Medium/High)
    - Impact (Low/Medium/High)
    - Mitigation Strategy (e.g., MFA, regular policy reviews, logging/alerting)
- Discussion of any dependencies or shared risks between AWS, Azure, and Fortinet components.
- Evidence of planning, such as risk register screenshots if you use a tool (optional but encouraged).

Deliverables:

Risk Assessment Document including:

- Complete risk table
- Written explanation of selected mitigation strategies
- Integration of risk management approach with overall project scope

Task 3: Part-B | Security Incident Analysis

Description:
Simulate and document a security incident scenario relevant to your multi-cloud deployment (for example, unauthorized access, security breach, misconfigured security group). Perform an analysis of how your team would detect, respond to, and remediate the incident.

What to Include:

- Description of the selected incident scenario
- Timeline of incident detection and response steps
- Roles and responsibilities in response (who does what)
- Logging and monitoring evidence (CloudWatch, CloudTrail, Azure Monitor, Fortinet logs)
- Plan for recovery and lessons learned

Deliverables:

- Incident scenario narrative
- Detection and response timeline
- Screenshots or sample logs
- Roles/responsibilities table
- Mitigation and recovery plan

Phase 4 | Prepare Project Documentation, Write Report and Conduct Verification

In this final phase, you will consolidate all work into professional documentation. You will also verify your implementation against project requirements and test your solution to ensure it meets security, availability, and functionality goals.

Task 4: Project Documentation, Report Writing, Testing and Verification

Description:
Produce a polished final report and evidence package demonstrating your complete multi-cloud project. Validate that your design meets Yoobee College's requirements for security, high availability, and cost efficiency.

What to Include:

- Executive Summary of the project
- Architecture diagrams (AWS, Azure, Fortinet integration) with final configurations
- Detailed implementation steps for AWS, Azure, and Fortinet (including screenshots and code/scripts)
- Results of testing (e.g., HTTPS access via Azure DNS, Fortinet security result, Load Balancing, Auto Scaling)
- Verification checklist mapping requirements to evidence
- Reflection on challenges, solutions, and team learning outcomes

Deliverables:

Submit a **single, well-organized PDF report** that includes the following:

Cover Page

- Project title
- Team members' full names and student IDs
- Date of submission

Executive Summary

- Brief overview of project goals, scope, and outcomes

Full Project Architecture and Design Documentation

- Final architecture diagrams (AWS, Azure, Fortinet integration)
- Detailed design decisions

Implementation Steps with Screenshots

- AWS, Azure, and Fortinet configurations
- CLI commands or code snippets if used
- Screenshots clearly labeled

Testing and Verification Results

- Evidence of secure HTTPS access
- VPN connectivity tests
- Load Balancer/Auto Scaling functionality
- Monitoring/logging validation

Risk Assessment and Incident Analysis Appendices

- Final risk assessment table with mitigation strategies
- Security incident scenario analysis with detection and response plan

References and Citations

- Any sources, tools, or templates used (APA or suitable academic style)

Marking Rubric

To pass this assessment, you must meet the requirements of each of the learning outcomes (irrespective of the numerical grade awarded).

Criterion		Evidence				
Task and Weightage		**A (80-100%)**	**B (65-79%)**	**C (50-64%)**	**D (40-49%)**	**E (0-39%**
Phase 1: (LO2) **Project Planning, Design, and Assignment of Group and Individual Roles** **Task-1: Project Planning**	**15%**	The submission exemplifies outstanding achievement, fully addressing all task requirements with high detail and precision. It is professionally structured, featuring clear headings, well-labelled tables, and comprehensible diagrams. Roles and responsibilities are realistic and well-distributed, reflecting strong expertise in AWS/Azure integration and security planning. Technical accuracy is exceptional, with thorough, realistic planning that anticipates risks and includes robust mitigation strategies. Communication planning demonstrates excellent team coordination and engagement. Overall, the work meets professional industry standards and provides an exemplary blueprint for implementation.	The submission satisfactorily meets requirements with minor gaps. It is well-organized, clearly articulated, and addresses all key task elements. Roles and responsibilities are appropriately assigned, though some minor imbalances or simplifications exist. Architecture diagrams and planning steps are clear and mostly complete but may lack finer detail. Risk management and communication strategies are relevant yet could benefit from deeper specificity. Technical inaccuracies are minimal and do not impact overall quality. This work is professionally suitable, requiring only minor revisions to align fully with industry standards.	The submission meets minimum task requirements but reveals clear limitations. Content covers required sections but tends to be basic or generic, lacking specific detail. Structure and formatting are inconsistent, affecting professionalism and readability. Roles and responsibilities are included but may be unevenly assigned or vaguely described. Architecture diagrams and planning checklists are present but simplistic or partially incomplete with limited explanation. Risk management and communication strategies exist but are underdeveloped and may not fully address project complexities. Technical errors or unrealistic assumptions appear but do not fundamentally undermine the submission's purpose. This work is acceptable for progression but requires significant improvement to meet industry standards.	The submission partially meets requirements but exhibits significant deficiencies. Content is frequently incomplete, unclear, or poorly organized, with many elements missing or superficially addressed. Roles and responsibilities are unrealistic, vague, or unevenly distributed, reflecting limited team coordination. Diagrams are often unclear, incomplete, unlabelled, or absent. Planning steps lack coherence and logical flow. Risk management and communication strategies are minimal, generic, or ineffective. Technical errors and unrealistic design choices are prevalent, undermining credibility. This work is unsuitable for professional or industry-standard use without major revision and substantial guidance.	The submission fails to meet minimum task requirements, with content that is missing, incoherent, irrelevant, or fundamentally flawed in understanding the planning process. Key sections are largely absent or severely incomplete, lacking meaningful planning, defined roles, or responsibilities. Diagrams, if present, are unintelligible or missing. Planning checklists, risk management, and communication strategies are inadequate or non-existent, providing no viable project path. The work demonstrates little to no grasp of AWS/Azure integration or secure cloud architecture principles. This submission is unacceptable for progression and requires comprehensive rework and substantial support to reach minimum standards.

Criterion		Evidence				
Task and Weightage		**A (80-100%)**	**B (65-79%)**	**C (50-64%)**	**D (40-49%)**	**E (0-39%**
Phase 2: (LO2, LO3, LO4, LO6) **Multi-Cloud Project Implementation Using AWS and Azure Services, with Security Incident Identification and Troubleshooting** **Task-2:** **Part-A | Project Implementation using Aws Cloud Services** **Part-B | Project Implementation using Azure Cloud Services** **Part-C | Multi-Cloud Security Integration**	**(50%)**	The submission demonstrates expert-level implementation across AWS, Azure, and multi-cloud security. Part A delivers a secure, professional AWS setup with comprehensive documentation and best practices. Part B presents a well-configured, secure Azure environment integrated seamlessly with AWS. Part C showcases robust multi-cloud security using Fortinet FortiGate, with thorough risk assessment and strong evidence of effective controls. Overall, the work reflects advanced proficiency in secure, multi-tier cloud architecture and integration.	The submissions deliver core AWS, Azure, and FortiGate components with minor gaps or errors. Configurations and security controls show solid understanding but may lack full optimization or detail. Documentation and evidence are generally clear but occasionally inconsistent or incomplete. Overall, each part demonstrates strong foundational proficiency and would require only modest refinements to meet professional standards.	The submissions address all key AWS, Azure, and security components at a basic or partial level. Configurations are often generic, incomplete, or simplified, with inconsistent or unclear documentation and evidence. Security best practices are only partially applied, and critical features like tagging, MFA, and detailed risk mitigation may be lacking. Overall, the work reflects foundational understanding but requires significant improvement to meet professional industry standards	The submissions are incomplete or significantly flawed across AWS, Azure, and security components. Key services are missing or misconfigured, with poor or disorganized evidence and documentation. Tagging and security practices are weak or absent, and VPN testing may be unsuccessful or undocumented. FortiGate integration is often non-functional or missing, and risk assessments are minimal or unrealistic. Overall, the work reflects limited understanding and requires major revision to achieve practical viability and professional standards.	The submissions fail to meet minimum requirements across all parts. For Part A, essential AWS components are largely missing or incorrect, with absent or irrelevant evidence, no tagging, and fundamental security misunderstandings. Part B lacks most required Azure elements, with insufficient documentation and flawed security practices, reflecting minimal grasp of Azure and AWS integration. Part C shows missing or incorrect security controls, absent FortiGate integration, and no meaningful risk assessment, indicating no substantive understanding of secure multi-cloud design or implementation
Phase 3: (LO3, LO4) **Risk Assessment and Security Incident Analysis** **Part-A | Risk Assessment and Mitigation Strategy** **Part-B | Security Incidents Analysis**	**(20%)**	Exceptionally thorough and structured risk assessment table with clear mitigation strategies. Security incident analysis is realistic, detailed, with strong detection, response and recovery plan. Includes clear roles and logs/screenshots.	Clear and structured risk assessment with mostly suitable mitigations. Incident analysis realistic but minor detail gaps. Good detection and response plan.	Adequate risk assessment but lacks detail or depth. Incident analysis generic or partially complete. Detection/response plan basic.	Poorly developed risk assessment and incident analysis. Major omissions or vague responses. Limited detection/response planning.	Little or no evidence of risk assessment or incident analysis.
Phase 4: (LO6) **Prepare Project Documentation, Write Report and Conduct Verification** **Task-4: Project Documentation, Report Writing and Verification**	**(15%)**	Professional, polished, well-structured report. Includes all required sections (cover page, executive summary, architecture diagrams, screenshots, risk assessment, incident analysis). Verification checklist clear. Demonstrates critical reflection	Well-organised report covering nearly all requirements with minor issues in structure or detail. Verification checklist mostly clear. Reflection present	Report covers most requirements but with incomplete sections or unclear presentation. Verification checklist basic or partial. Limited reflection.	Incomplete, poorly structured report with major omissions. Weak or unclear verification. Little reflection	Little or no evidence of documentation or verification.